UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/527,570	03/10/2005	Markus Bockes	WACHP006	7328

25920 7590 12/16/2008

MARTINE PENILLA & GENCARELLA, LLP
710 LAKEWAY DRIVE
SUITE 200
SUNNYVALE, CA 94085

EXAMINER	
PACHURA, REBECCA L	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
12/16/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/527,570	BOCKES ET AL.	
	Examiner	Art Unit	
	Rebecca L. Pachura	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 September 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,14-20,22-32 and 34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 14-20, 22-32, and 34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 March 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/01/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement filed 12/01/2008 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because "item T does not have a publication date associated with it". It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

Specification

2. The objection to the abstract is withdrawn based on the new abstract submitted on 09/29/2008.

Claim Objections

3. The objections to claims 14-26, 28, 29, 31, 33, and 34 are withdrawn based on the amendments submitted on 09/29/2008.

Status of Claims

4. **Claims 1, 14-20, 22-32, and 34 are pending in this Office Action.**

Claims 1, 14-20, 22-32, and 34 are amended.

Claims 21 and 33 are canceled.

Response to Amendment

5. **The 35 U.S.C. 112, second paragraph rejection on claims 17 and 25 is withdrawn based on the applicant's amendments submitted on 09/29/2008. The 35 U.S.C. 101 rejection on claims 27-31 is withdrawn. The 35 U.S.C. 101 rejection on claims 1, 14-20, 22-26, 32, and 34 is not withdrawn.** The amendment to independent claims 1 and 32, "wherein the cryptographic calculation is one of a decryption in an RSA method and a signature generation in an RSA method" does not fix the lack of a result in the limitations of the claims it just adds another limitation.

Response to Arguments

6. Applicant's arguments with respect to claims 1, 14-20, 22-32, and 34 have been considered but are moot in view of the new ground(s) of rejection.

Applicant's Invention as claimed:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 1, 14-20, 22-32, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over WO 0161918 (US 20030159036) (Walmsley) (Applicant's IDS) in view of US 20030097628 (Ngo) and in view of US 6965673 (Boneh).**

As to claim 1, Walmsley discloses (Currently amended) a method for protected execution of a cryptographic calculation, in which a key with at least two key parameters is drawn on, wherein an integrity check of the key is performed (Walmsley page 23, paragraphs 0628 and 0629 and page 24, paragraph 0652), in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter (Walmsley page 24, paragraph 0657). Walmsley does not explicitly teach and wherein the cryptographic calculation is one of a decryption in an RSA method and a signature generation in an RSA method.

However, Boneh discloses wherein the cryptographic calculation is one of a decryption in an RSA method and a signature generation in an RSA method (Boneh column 7, lines 30-37).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Boneh because RSA decryption and signature generation are well know cryptographic calculations and to use these protected calculations would increase there security (Boneh column 7, lines 30-37).

As to claim 14, Walmsley discloses (Currently amended) a the method as claimed in claim 1, wherein in the integrity check it is determined whether the value of at least one key

parameter is contained in a range of valid values, wherein the range is non-contiguous in that it has a plurality of gaps (Walmsley page 40, paragraph 0998).

As to claim 15, Walmsley discloses (Currently amended) ~~a~~ the method as claimed in claim 1, wherein in the integrity check it is determined whether at least two key parameters are in a predetermined relationship to one another (Walmsley page 40, paragraph 0998).

As to claim 16, the modified Walmsley discloses (Currently amended) ~~a~~ the method as claimed in claim 1. The modified Walmsley does not explicitly teach wherein the integrity check includes a multiplicative operation, in particular a divisibility test.

However, Ngo discloses wherein the integrity check includes a multiplicative operation, in particular a divisibility test (Ngo page 1, paragraph 0009).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Ngo because to use a divisibility test for an integrity check is a cheaper and a faster calculation (Ngo page 1, paragraph 0009).

As to claim 17, the modified Walmsley discloses (Currently amended) ~~a~~ the method as claimed in claim 1. The modified Walmsley does not explicitly teach wherein in the integrity check it is checked whether at least one of the key parameters is evenly divisible by ~~the~~ a safeguard value.

However, Ngo discloses wherein in the integrity check it is checked whether at least one of the key parameters is evenly divisible by ~~the~~ a safeguard value (Ngo page 2, paragraph 0026).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Ngo because again the divisibility check is cheaper and

faster as well as if you use a predetermined value it adds to the assurance that there are no errors or whether or not corruption has occurred (Ngo page 2, paragraph 0026).

As to claim 18, the modified Walmsley discloses (Currently amended) ~~a~~ the method as claimed in claim 1. The modified Walmsley does not explicitly teach wherein in the integrity check it is checked whether at least one value which differs from one of the key parameters by a multiple of a safeguard value is evenly divisible by the safeguard value.

However, Ngo discloses wherein in the integrity check it is checked whether at least one value which differs from one of the key parameters by a multiple of a safeguard value is evenly divisible by the safeguard value (Ngo page 2, paragraph 0026).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Ngo because to add another multiple as a blinding factor increases the security of the protected calculation (Ngo page 2, paragraph 0026).

As to claim 19, Walmsley discloses (Currently amended) ~~a~~ the method as claimed in claim 1, wherein in the integrity check a checksum stored with the key parameters is compared with a checksum newly calculated after passing of the key parameters (Walmsley page 13, paragraphs 0036-034 and page 14, paragraph 0036).

As to claim 20, Walmsley discloses (Currently amended) ~~a~~ the method as claimed in claim 1, wherein, to check the integrity, important parameters to be passed are multiply passed and checked for identity after passing (Walmsley page 13, paragraphs 0036-034 and page 14, paragraph 0036).

As to claim 22, the modified Walmsley discloses (Currently amended) ~~a~~ the method as claimed in claim ~~21~~ 1. The modified Walmsley does not explicitly teach wherein the RSA method is an RSA-CRT method.

However, Boneh discloses wherein the RSA method is an RSA-CRT method (Boneh column 7, lines 20-65).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Boneh because the RSA-CRT is a well know cryptographic calculation and to use these protected calculations would increase there security (Boneh column 7, lines 20-65).

As to claim 23, the modified Walmsley discloses (Currently amended) ~~a~~ the method as claimed in claim ~~21~~ 1. The modified Walmsley does not explicitly teach wherein in the cryptographic calculation at least one exponentiation operation is performed and in the integrity check it is checked whether the exponent used in the exponentiation operation is evenly divisible by a safeguard value.

However, Ngo discloses wherein in the cryptographic calculation at least one exponentiation operation is performed and in the integrity check it is checked whether the exponent used in the exponentiation operation is evenly divisible by a safeguard value (Ngo page 2, paragraph 0026).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Ngo because the divisibility check is cheaper and faster as well as if you use a predetermined value it adds to the assurance that there are no errors or whether or not corruption has occurred (Ngo page 2, paragraph 0026).

As to claim 24, the modified Walmsley discloses (Currently amended) ~~a~~ the method as claimed in claim 23. The modified Walmsley does not explicitly teach wherein in the cryptographic calculation an exponent blinding method is applied for protection against spying.

However, Boneh discloses wherein in the cryptographic calculation an exponent blinding method is applied for protection against spying (Boneh column 17, lines 41-46).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Boneh because to add another multiple as a blinding factor increases the security of the protected calculation (Boneh column 17, lines 41-46).

As to claim 25, Walmsley discloses (Currently amended) ~~a~~ the method as claimed in claim ~~21~~ 1, wherein the prime factors of the RSA method are multiplied by a masking parameter and the error freedom of the calculation sequence is checked by an equality check modulo the masking parameter (Walmsley page 4, paragraph 0089).

As to claim 26, the modified Walmsley discloses (Currently amended) ~~a~~ the method as claimed in claim 1. The modified Walmsley does not explicitly teach wherein at least one key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check.

However, Ngo discloses wherein at least one key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check (Ngo page 1, paragraph 0009 and page 2, paragraph 0026).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Ngo because the divisibility check is cheaper and faster as well as if you use a predetermined value it adds to the assurance that there are no errors or

whether or not corruption has occurred and to add another multiple as a blinding factor increases the security of the protected calculation (Ngo page 1, paragraph 0009 and page 2, paragraph 0026).

As to claims 27-32 and 34, claims 27-32 and 34 encompass the same scope of the invention as those of claims 1 and 26 with the additions of "computer readable storage medium" (Walmsley page 53, paragraph 1297) and portable data carrier (Walmsley page 4, paragraph 0098: smart card).

Remarks

8. Applicant has presented amendments for the 35 U.S.C. 112, second paragraph rejection and has canceled 2 claims. Applicant has made arguments for the rest of the response, see below.

The Applicant Argues:

In view of the foregoing, it cannot reasonably be said that keys K_1 and K_2 are two key parameters of a key, as specified in the claimed subject matter. The recitation of "a key with at least two key parameters" requires that the key parameters in some way form an overall key for the cryptographic calculation. This is not the case in the Walmsley reference, where the two keys K_1 and K_2 are entirely distinct and are used in two different cryptographic calculations. Moreover, Walmsley does not disclose that any one of the two keys K_1 and K_2 has at least two key parameters. Thus, the Walmsley reference does not disclose (or suggest) a key with at least two key parameters, as specified in the claimed subject matter.

In response, the examiner respectfully submits:

A parameter is any factor that helps define a system it does not necessarily mean it forms the overall key. With that said Walmsley does teach at least two key parameters a random number R and a memory vector M (Walmsley page 23, paragraphs 0628 and 0629).

The Applicant Argues:

Second, the Walmsley reference does not disclose (or suggest) preventing a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter. As discussed above, the Walmsley reference does not disclose a key with at least two key parameters. Thus, the Walmsley reference necessarily does not disclose preventing a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter. However, even if, for the sake of discussion, the keys K_1 and K_2 of Walmsley were considered to be the equivalent of the claimed key parameters, the Walmsley reference still would not disclose this feature. As described above, the keys K_1 and K_2 are entirely separate. They are randomly generated independently from one another, and they are used in distinct operations. As such, any disturbance of one of the keys and the corresponding computation would not allow an attacker to draw any conclusion about the other key, and nothing in the Walmsley reference teaches or suggests such a possibility.

In response, the examiner respectfully submits:

Walmsley does teach preventing a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter (Walmsley page 23-24, paragraph 0657).

The Applicant Argues:

Third, the Walmsley reference does not disclose (or suggest) that the cryptographic calculation is one of a decryption in an RSA method and a signature generation in an RSA method. On page 9 of the Office Action (in connection with the discussion of claim 21), the Examiner acknowledges that "Walmsley fails to teach wherein the cryptographic calculation is one of a decryption in an RSA method and a signature generation in an RSA method." Thus, the Walmsley reference does not disclose (or suggest) this feature of the presently claimed subject matter.

In response, the examiner respectfully submits:

This argument is moot based on the new grounds of rejection.

The Applicant Argues:

Applicants have amended each of independent claims 27, 30, and 32 along the same lines that claim 1 has been amended. As such, the arguments set forth above regarding present claim 1 also apply to present claims 27, 30, and 32. Accordingly, independent claims 1, 27, 30, and 32, as amended herein, are patentable under 35 U.S.C. § 102(b) over Walmsley. Claims 14, 15, 19,

and 20, each of which depends from claim 1, are likewise patentable under 35 U.S.C. § 102(b) over Walmsley for at least the same reasons set forth above regarding claim 1.

In response, the examiner respectfully submits:

Please see arguments above. The dependent claims are rejected as depending from rejected independent claims.

The Applicant Argues:

The Walmsley reference is concerned with a validation protocol that uses symmetric cryptographic functions (see Paragraphs [0335]-[0346]). On the other hand, the Boneh reference is concerned with asymmetric cryptographic functions according to the RSA method. It is well known to those skilled in the cryptographic arts that symmetric and asymmetric cryptographic functions constitute vastly different fields and that concepts used in one of these fields cannot be interchangeably used in the other field. As such, one having ordinary skill in the art would not have had a reasonable expectation that any meaningful result could be obtained by combining the Walmsley and Boneh references in the manner proposed by the Examiner.

In response, the examiner respectfully submits:

Walmsley does disclose asymmetric cryptographic functions please see Protocol C2 (Walmsley page 23-24, paragraphs 0623-0670).

The Applicant Argues:

The attack contemplated by Boneh is a so-called fault attack in which the calculation steps of exactly one branch of the RSA calculation are disturbed by an external influence such

as, for example, heat or radiation or electrical pulses. This kind of attack, which is also known by the name "Bellcore attack," is acknowledged and discussed in detail in Paragraphs [0005] and [0006] of the subject application. However, as set forth in Paragraph [0010] of the subject application, the claimed subject matter is based on the insight that an attack similar to the Bellcore attack is possible not only by interfering with the calculation process during the cryptographic calculation, but also by supplying the cryptographic calculation with incorrect key parameters. The claimed subject matter strives to provide protection against these kind of attacks, i.e., protection against attacks "in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter," as specified in the present claims. The Boneh reference does not disclose or fairly suggest this claimed feature.

In response, the examiner respectfully submits:

Please see arguments above.

The Applicant Argues:

The Boneh reference also does not disclose or suggest the performing of an integrity check of the key. The primary teaching of Boneh is a description of various attack schemes. The Boneh reference discusses possible countermeasures to such attacks only in passing in column 17 of the reference. The proposed countermeasures include checking the output of a computation before releasing it, checking intermediate results held in internal registers of the cryptography device, and using blinding operations. As such, Boneh does not teach or fairly suggest the performing of an integrity check of the key, as specified in the presently claimed subject matter.

In response, the examiner respectfully submits:

Please see arguments above.

Based on the examiner's arguments claims 1, 14-20, 22-32, and 34 are rejected under 35 U.S.C. 103(a).

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Rebecca L. Pachura whose telephone number is (571) 270-3402. The examiner can normally be reached on Monday-Thursday 10:00 am-8:00 pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Rebecca L Pachura/
Examiner, Art Unit 2436

/Carl Colin/
Primary Examiner, Art Unit 2436